Version Number: 01-2019

U.S. Department of Commerce
National Institute of Standards and Technology
(NIST)

Privacy Threshold Analysis
for the
150-01 Office of Safety, Health, and Environment

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 150-01

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system
b) System location
c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
d) The purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, use, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from the system

The Office of Safety, Health, and Environment (OSHE) supports NIST in carrying out its mission safely and in maintaining safety as an integral core value and vital part of the NIST culture. The OSHE information system supports this role and includes the following components:

- **The Radiation Monitoring System (RMS) is used to monitor radioactive sources above a certain level. The RMS has detectors, processors, cameras, and network connectors monitoring sensitive equipment and their surrounding physical locations. The monitoring provides unidirectional information to Physical Security consoles.**
- **The Health Physics System (a.k.a., HAPPY) provides inventory of radioactive material, ionizing machines, radiation equipment, physical radiation laboratories,**

safety training, and tracking of radiation doses that NIST staff receive. An additional system, AREV, has the same functionality, but serves as an archive from 2006 and prior.

- **Health Unit applications track NIST staff health scheduling (e.g., frequency) and audiometer and spirometer test results.**
- **The Health Unit Intake procedures require completion of an intake form from any NIST staff or visitor for identification purposes, and health information.**
-

a. Whether it is a general support system, major application, or other type of system
150-01 is a General Support System.

b. System location
The components are located at the NIST Gaithersburg, Maryland and Boulder, Colorado facilities within the continental United States.

c. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The RMS systems can only communicate with systems located in the physical security guard's offices via a private network in Buildings 101 and 318 over OSHE's isolated Research Equipment Network.

All system connectivity to Happy and all the Health Unit data is via TCP/IP across the NIST Network Infrastructure (SSP 181-04) to the encrypted file share (184-12). The NIST Network Infrastructure system provides all services for physical cabling, network frame synchronization/flow control/error checking, routing, switching, and DNS. Data is encrypted with FIPS 140-2 compliant technologies in transit and at rest. The Health Unit intake forms are standalone and not interconnected.

d. The purpose that the system is designed to serve
The 150-01 system contains the hardware and software required by the NIST Office of Safety, Health, and Environment (OSHE) staff to provide the Safe support to help reduce safety, health, and environmental (SH&E) risks at NIST by planning, developing and maintaining, supporting the implementation of, overseeing compliance with, and continually improving NIST's SH&E programs. In doing so, OSHE will enable NIST to carry out its mission effectively and efficiently while protecting the worker, the public, and the environment and complying with applicable laws and regulations. Additionally, the 150-01 system includes safety-related applications that are available to and can be used by all NIST staff in support of the OSHE and NIST mission.

e. The way the system operates to achieve the purpose
The RMS provides continuous monitoring capabilities via a live video feed for physical security to prevent unauthorized access to radioactive material.

Access to and inventory of radioactive material are stored in a database application, HAPPY. Owners of material access and update the database via secured, authorized computers.

Physical test results are stored in applications via specialized software attached to diagnostic machines. When an existing patient visits the Health Unit, a patient's file may be retrieved by name.

f. A general description of the type of information collected, maintained, used, or disseminated by the system
RMS provides a live feed. They have detectors, processors, cameras and network connectors. There are no input/output devices on the systems; they feed and are controlled by systems located in the physical security guard's office in Buildings 101 and 318. They are on a dedicated private network, cannot communicate with each other and only to the Emergency Service Division's consoles. The RMS systems record all camera activity to a DVR in the ESD space. DVR will recycle and overwrite previous activity unless an alarm sounds. It will then prevent data to be overwritten.

HAPPY collects inventory and dosimetry results of radioactive material via the owner's input into the database. The SSNs of material owners are required for reporting purposes to the Nuclear Regulatory Commission to retain our license to work with radioactive material.

Health Unit – The Gaithersburg Health Unit (HU) provides medical assistance and tracking of Occupational Health Records in addition to Personal Health Records. Each patient fills in an Intake Forms (NIST 986) that contains both Personally Identifying Information including Social Security Number and Date of Birth as well as Health Information. These records are stored in hard copy only and only within the HU in locked storage cabinets. There are two managed desktop Windows machines attached to medical equipment that collect test results for patients: spirometer and audiometer. There are two Access databases that store what individuals participate in certain medical programs that contain Date of Birth to track when tests are required. These test results and databases are stored on an encrypted shared drive maintained by OISM (SSP 184-12).

g. Identify individuals who have access to information on the system
RMS feeds are only made available to Emergency Service Divisions employees. In the event of an incident the recordings would be made available to other law enforcement entities.

All PII and PHI data is shared minimally. In support of licensing, NIST is required to share information in HAPPY with the Nuclear Regulatory Commission (NRC).
Health Unit Intake procedures provide patients an explanation of how information collected is used. Occupational Health Records (OHR) are owned by NIST, but regulated by the Occupational Safety and Health Administration, and shared with other internal DOC and NIST business units. Personal health information is shared as a circumstance or situation warrants, only with the consent of the patient.

h. How information in the system is retrieved by the user
The RMS is viewed by NIST police on a continuous basis.

HAPPY data is retrieved by authorized individuals by opening the database and retrieving the source by identifier. Source owners can be retrieved by name. Health Unit information is retrieved by patient name.

i. How information is transmitted to and from the system
RMS data is only transmitted over an isolated network and encrypted during transit. Happy and Health Unit data are transmitted via encrypted channels.

Questionnaire:

1. The status of this information system:
   This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
   NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Activities
Other activities which may raise privacy concerns:

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
   As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?
   As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

   The IT system collects, maintains, or disseminates PII about:

   If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

Is a PIA Required?	**Yes**

CERTIFICATION

___X_ I certify the criteria implied by one or more of the questions above **apply** to the 150-01 Office of Safety, Health, and Environment and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the 150-01 Office of Safety, Health, and Environment and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Banovic, Stephen

Signature of SO: STEPHEN BANOVIC Digitally signed by STEPHEN BANOVIC Date: 2020.08.26 07:22:12 -04'00' Date: _____

Name of Co-Authorizing Official (Co-AO):

Mackey, Elizabeth

Signature of Co-AO: Mackey, Elizabeth A. Dr. (Fed) Digitally signed by Mackey, Elizabeth A. Dr. (Fed) Date: 2020.09.15 13:15:39 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Glenn, K. Robert

Signature of ITSO: KENNETH GLENN Digitally signed by KENNETH GLENN Date: 2020.08.19 07:52:47 -04'00' Date: _____

Name of Authorizing Official (AO):

Sastry, Chandan

Signature of AO: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2020.09.10 13:16:37 -04'00' Date: _____

Name of Privacy Act Officer (PAO):

Fletcher, Catherine

Signature of PAO: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2020.08.24 12:30:58 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO):

Schiller, Susannah

Signature of BCPO: SUSANNAH SCHILLER Digitally signed by SUSANNAH SCHILLER Date: 2020.08.19 08:47:06 -04'00' Date: _____